Ashwood Advisors, LLC®

5 North Meadows Road ● Medfield, MA ● (508) 359-9442 ● GeremiaInvestments.com

Truth, Knowledge, Experience *1st Quarter 2017*

Financial New Year's Resolutions: Using Tech to Stay on Track

Presented by Stephen Geremia

The New Year is symbolic in many respects. It gives you a chance to start fresh and set some goals that can improve your life in ways large and small. But if you're like many people, familiar resolutions like "lose weight" or "go to the gym" slowly fade into darkness by mid-February, leaving you feeling disappointed in yourself.

This year, why not try focusing on a different aspect of your life—your finances? Instead of vowing to slim down, you can work on fattening your wallet with some tech-related resolutions. (And they're probably more sustainable than waking up at 5:00 A.M. to hit the gym before work!)

Making your finances a priority in 2017

Being aware of your finances, staying on budget, and spending less are easy resolutions to adopt. All you have to do is say these three phrases out loud: "I am going to be more cognizant of my finances this year," "I am going to be extremely frugal this year," and finally, "I am not going to spend as much as I did last year." That's it—you're done with your New Year's resolutions.

Only kidding! Simply making these resolutions and hoping for the best isn't going to work. You need to take a more tactical approach to bettering your finances. Fortunately, a number of smartphone apps and other tech tools are available to help you be more disciplined in your budgeting and spending, turning those resolutions into worthwhile, maintainable habits.

There's an app for that!

Mint. One of the first budgeting apps available was Mint—a program that allows you to see all of your accounts in one place. By creating a log of your purchases, the app helps you keep track of your spending. After building up a large enough sample size of your purchases and transactions, Mint will even start categorizing them automatically. The app will alert you when bills are due and if any fees have been assessed on your linked accounts. In addition, Mint monitors your credit card balance relative to your spending limits, and it will warn you if any balances exceed a certain threshold of available credit.

Digit. Would you like to be better about putting money into your savings account on a regular basis? If so, then Digit could be the tech solution for you. This service, which also includes an app, monitors your spending patterns via your checking account to calculate a suitable amount to transfer to savings. You also have the option of manually adding money to your savings account by initiating transfer requests. Plus, as a Digit user, you'll receive weekly reports via text message to keep you abreast of your current balances.

Prosper Daily. Given the growing threat of cybercrime, you may be worried about protecting your identity and making sure no one else has access to your hard-earned money. Prosper Daily helps deter scammers, targeting activity that doesn't seem quite right on your linked accounts. It can even track your GPS location to see if your cards are being used elsewhere. For instance, if your card is used and it doesn't match up to your current location,

Hi Everyone,

The recent rate hike by the Fed has been anticipated by the market for some time and has been taken in stride. Republicans and Democrats alike want massive infrastructure spending, The main question is how it gets paid for.

Sincerely,
Steve Geremia

In This Issue:

- **Financial New Year's Resolutions: Using Tech to Stay on Track**
- **To Pay or Not to Pay: How to Survive a Ransomware Attack**

you'll receive an alert via the app to notify you of this discrepancy. Then, you can dispute the charge right from your phone. To provide even more protection, it also performs regular "black market surveillance"—scanning websites and hacker forums to ensure that your personal information is not being traded, bought, or sold.

Mint Bills. If you need help keeping track of when bills are due during the course of the month, this app is for you. With Mint Bills, you can see all of your account balances, transactions, and the due dates of certain bills. It allows you to view your bills (e.g., credit card, insurance, and utilities) in one centralized place, includes a reminder system to help you avoid late fees, and lets you pay bills directly from the app.

Toshl. Skeptical of linking your whole world to your smartphone? More of a do-it-yourselfer when it comes to budgeting and spending? If you're not comfortable uploading *all* of your information and account numbers to the digital world, Toshl may be the right fit for you. The app allows you to manually enter and categorize transactions as you see fit. It will also notify you when bills are due, analyze trends based on your past spending habits, and allow you to easily export your data to an Excel or PDF file.

Cheers to better financial fitness

In this day and age, using technology to your advantage is a must. With the help of apps available right at your fingertips, you can ensure that you stick to your spending and budgeting resolutions. Here's to greater financial knowledge, organization, and prosperity in the New Year!

The trick is to stop thinking of it as "your" money.—IRS auditor

To Pay or Not to Pay: How to Survive a Ransomware Attack

Presented by Stephen Geremia

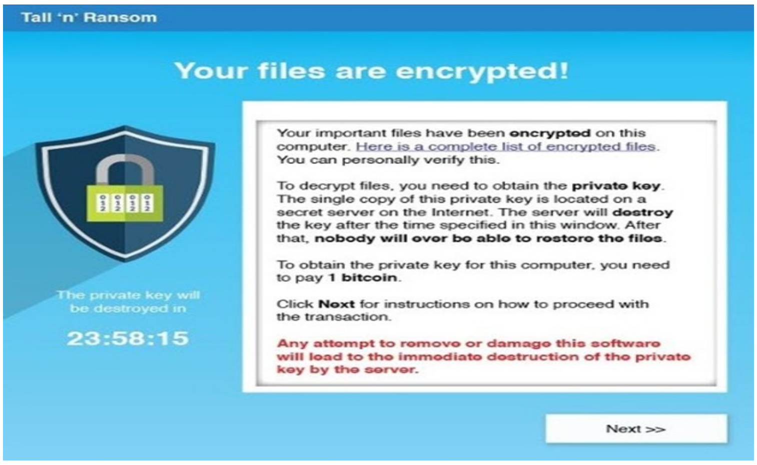
Imagine this: You open an e-mail that seems to come from Google, prompting you to click a link to reset your password. But when you click, a mysterious .exe file downloads and launches. Slowly, all the files on your desktop turn into white paper icons, and the names of all your files turn into scrambled nonsense.

What is happening here? Unfortunately, you've probably fallen victim to a ransomware attack.

The threat defined

Ransomware, as defined by Trend Micro, is "a type of malware that prevents or limits users from accessing their system . . . unless a ransom is paid." Although the term may be new to you, ransomware attacks happen every day. In fact, according to Kaspersky Lab's Securelist, 2.3 million Internet users encountered ransomware between April 2015 and March 2016, and Armada Cloud reports that the volume of attacks grew by 13 percent between August and October 2016.

In the event that a ransomware attack happens to you, it's likely that something much like the scenario mentioned above will unfold. Here's an example of what you might see on your computer screen:



Your files are encrypted!

Your important files have been **encrypted** on this computer. Here is a complete list of encrypted files. You can personally verify this.

To decrypt files, you need to obtain the **private key**. The single copy of this private key is located on a secret server on the Internet. The server will **destroy** the key after the time specified in this window. After that, **nobody will ever be able to restore the files**.

To obtain the private key for this computer, you need to pay **1 bitcoin**.

Click **Next** for instructions on how to proceed with the transaction.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

The private key will be destroyed in

23:58:15

Now what?

So, do you pay the ransom or simply wait for the countdown to end? Before deciding, you might try searching online for a free tool that can decrypt your files. But keep in mind that the chances of success are extremely slim. Even if a solution to a previous type of ransomware is available, attackers learn from their mistakes and have likely used a more advanced form of the scheme on you.

You might also consider calling law enforcement. Unfortunately, there's very little that the FBI, for example, can do to resolve an individual ransomware incident. But reporting the crime can help put it on the authorities' radar, so they can work on a solution for future cases.

Most of the time, it all comes down to two choices: either you pay the ransomware fee or you don't.

You pay. One bitcoin equals $778 (at the time of this writing), so paying the ransom may be worth it to you, depending on what those files contain. You hit the Next button and follow the instructions to pay your attacker. What happens now?

- **Outcome 1: You get your files back.** Time to celebrate? Not so fast. From the cyber criminal's perspective, he or she just found a paying customer. Now you're a prime target for another ransomware attack.
- **Outcome 2: You don't get your files back.** Remember: you have no leverage. No one is forcing the criminals to hold up their end of the deal. Even if the attackers are "honorable," you can never be sure that the ransomware will keep your files intact.

You don't pay. Maybe you think the attacker is bluffing. (Hint: If you can't access your files, the attacker *isn't* bluffing.) Or maybe you've decided that the price tag for your data is too high.

- **Outcome 1: You're granted a time extension . . . and a price change.** Some attackers penalize you for waiting up to their deadline and then not paying. They give you a second chance but increase the ransom. Others realize that you won't take the bait, so they cut you a deal in an attempt to take what they can get. If so, you'll be back to deciding between paying and not paying.
- **Outcome 2: You don't get your files back**. On the bright side, you didn't contribute to one of the worst cyber threats we're facing today. Plus, those attackers won't see you as a receptive victim and may leave you alone in the future.

The best strategy: be prepared!

In the end, it's your decision. It all depends on how much you think your data is worth, as well as how much you trust that the attackers will stick to their end of the bargain. To give you some insight into the choices others are making, a recent Symantec report found that only 3 percent of victims pay the ransom.

Fortunately, there are three relatively simple precautions you can take to prevent such a costly scenario.

1) Back up your data regularly. Let's say that you back up your files every Sunday night. If you receive a ransomware threat on—worst-case scenario—a Sunday afternoon, you'll lose only a week's worth of data. If you would like to start backing up your files, you'll have to take the time to devise your own schedule and method. When establishing a backup plan, remember to keep these two things in mind: **Regularly test your backups.** You'd be surprised how many people wait until an attack or hard drive failure before they restore a backup for the *first* time, only to find that it doesn't work!
Store your backups separately from your computer. If backup media is connected to your system during an attack, your backup data could be targeted as well.

2) Be wary of phishing. Approximately 91 percent of cyber attacks start as phishing scams, according to *Wired*. When checking e-mail, remember to:

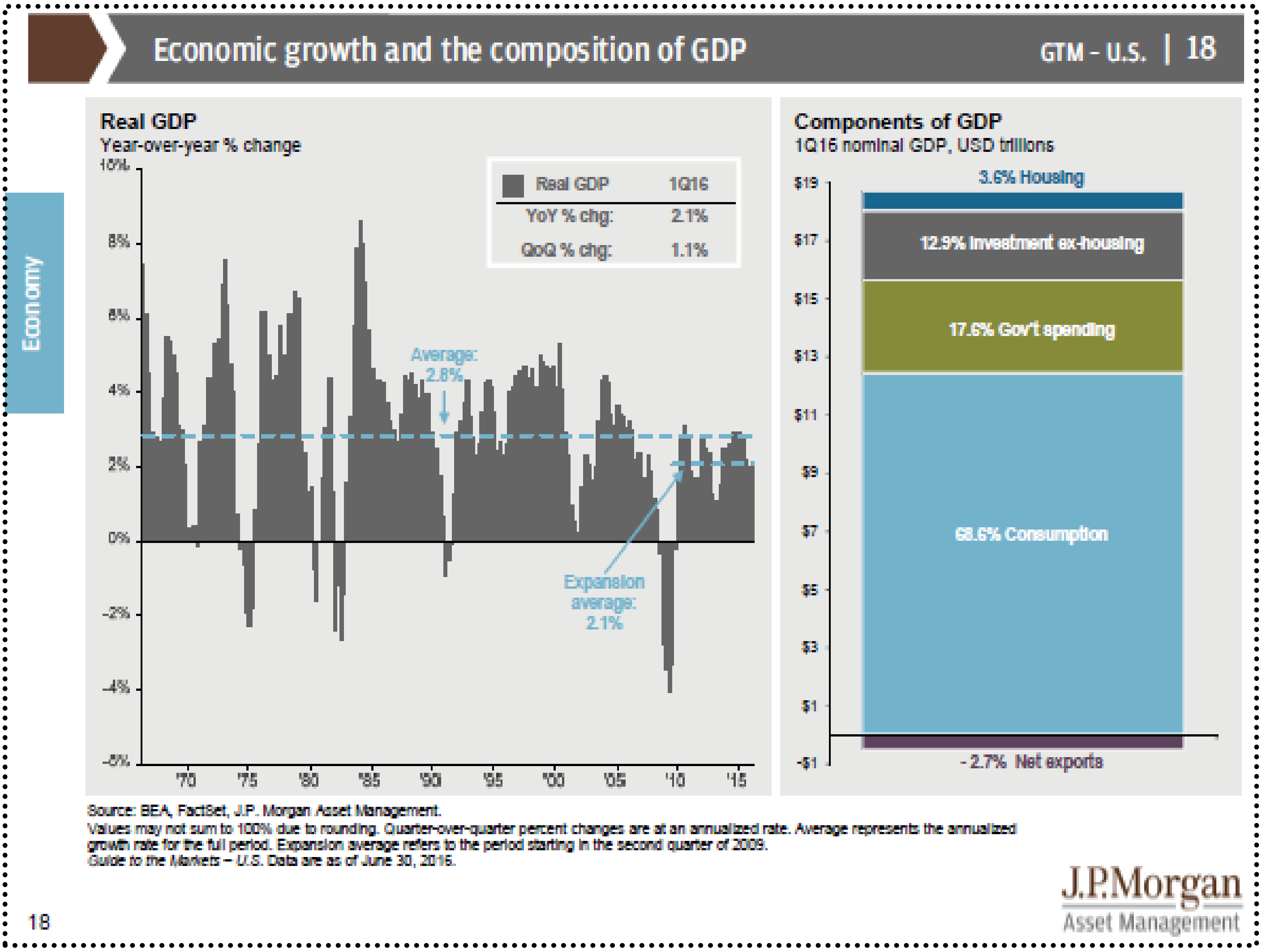
"My formula for success is to rise early, work late and strike oil" - JP Getty

- Hover over all links to verify that they’re safe
- Avoid clicking links whenever possible by typing URLs directly into your browser
- Delete any suspicious e-mails

3) Update your systems ASAP. Attackers know the vulnerabilities of yesterday’s technology. The longer you avoid regular updates, the more time attackers have to exploit those vulnerabilities.

Most of us haven’t experienced ransomware, but as the number of attacks increases, so does the probability of becoming a victim. If the day comes when it does happen to you, will you have a plan for handling the situation?

Intaxacation: Euphoria at getting a refund from the IRS, which lasts until you realize it was your money to start with.—From a Washington Post word contest



Economic growth and the composition of GDP

GTM – U.S. | 18

Economy

Real GDP

Year-over-year % change

Real GDP	1Q16
YoY % chg:	2.1%
QoQ % chg:	1.1%

Components of GDP

1Q16 nominal GDP, USD trillions

Source: BEA, FactSet, J.P. Morgan Asset Management.

Values may not sum to 100% due to rounding. Quarter-over-quarter percent changes are at an annualized rate. Average represents the annualized growth rate for the full period. Expansion average refers to the period starting in the second quarter of 2009.

Guide to the Markets – U.S. Data are as of June 30, 2016.

18

J.P.Morgan Asset Management

5 North Meadows Road · Medfield, MA 02052 · Tel: 508-359-9442 · Fax 508-359-2494 · Email: sgeremia@geremiainvestments.com
securities offered through commonwealth financial network, member finra/sipc, a registered investment adviser. advisory services offered through ashwood advisors, llc® are separate and unrelated to commonwealth

Ashwood Advisors, LLC®. A Registered Investment Advisor. All Rights Reserved.